PCT/DE 00/00157

BUNDESREPUBLIK DEUTSCHLAND

DE 00/00157

NIF

EJU

09/889730

Bescheinigung

Die ROBERT BOSCH GMBH in Stuttgart/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Steuergerät zur Steuerung sicherheitskritischer Anwendungen"

am 20. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 05 B, G 06 F und G 01 R der Internationalen Patentklassifikation erhalten.

München, den 29. Februar 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Wallner

Aktenzeichen: 199 02 031.0

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

A 9161
06.90
11/98

R. 32510

17.12.1998
Robert Bosch GmbH , 70469 Stuttgart

Steuergerät zur Steuerung sicherheitskritischer Anwendungen

Die vorliegende Erfindung betrifft ein Steuergerät zur Steuerung sicherheitskritischer Anwendungen mit einem Mikrocomputer (MC), einer Überwachungseinheit (Check Unit, CU) und Peripherieschaltungen (Input Output, IO). Die Erfindung betrifft außerdem ein Verfahren zum Überprüfen eines Mikrocomputers (MC) eines Steuergeräts zur Steuerung sicherheitskritischer Anwendungen, das den Mikrocomputer (MC), eine Überwachungseinheit (Check Unit, CU) und Peripherieschaltungen (Input Output, IO) aufweist.

Stand der Technik

In Steuergeräten, die sicherheitskritische Anwendungen oder Funktionen steuern bzw. regeln, müssen Fehler des Mikrocomputers (MC) bzw. eines Prozessors des Mikrocomputers durch Überwachung erkannt werden. Solche Steuergeräte mit Sicherheitsaufgaben werden bspw. für Antiblockiersysteme, für Antriebsschlupfregelsysteme und/oder für Fahrdynamikregelsysteme eingesetzt. Die sicherheitskritischen Anwendungen, die von dem Steuergerät gesteuert werden, sind über die Peripherieschaltungen mit dem Steuergerät verbunden. Bei Einrechner-Steuergeräten sind Verfahren mit einem Selbsttest, Plausibilitätsüberwachung und Watch-Dog bekannt.

Zur Prüfung von CMOS-Bausteinen (integrierte Schaltkreise,

IC) beim Hersteller werden Verfahren und Meßgeräte zur Messung des Ruhestromes eingesetzt. Der Hintergrund des sog. Ruhestromtestes besteht darin, daß in einem digitalen CMOS-Baustein in rein statischer Logik fast die gesamte Verlustleistung während der Schaltvorgänge in seinem Inneren entsteht. Im Ruhezustand beschränkt sich der Stromfluß auf winzige Leckströme, sowie Ströme durch Pullup- oder Pulldown-Widerstände an den Eingängen und externe Lasten an den Ausgangs-Treibern. Viele herstellungsbedingte Fehler führen zu einer verstärkten Leitfähigkeit zwischen der positiven und negativen Versorgungsspannung. Werden solche defekten Bereiche (Punktdefekte) der Schaltung aktiviert, führt dies zu einem sprunghaften Anstieg der Stromaufnahme. Durch eine hochgenaue Messung der Stromaufnahme während des Testvorgangs und einem Vergleich mit entsprechenden Sollwerten können solche Fehler festgestellt werden. Wie schon erwähnt, macht man sich eine solche Ruhestrommessung bei der Produktion von CMOS-Bausteinen zunutze, um nach dem Herstellungsprozeß die fehlerhaften Bausteine auszusortieren.

Aus dem Stand der Technik ist es bekannt, das bei der Produktion von Rechnerbausteinen bekannte Ruhestrom-Testverfahren auch bei Steuergeräten der eingangs genannten Art zur Überprüfung der Rechnerbausteine während ihres Normalbetriebs einzusetzen, um die häufigsten Fehler in den Rechnerbausteinen, insbesondere in dem Mikrocomputer (MC), bspw. Haftfehler (Stuck-at), Brückenfehler (Bridging) und/oder Unterbrechungsfehler (Stuck-Open), detektieren zu können.

Aus dem Stand der Technik ist es weiterhin bekannt, bei Steuergeräten der eingangs genannten Art zur Erhöhung der Fehlersicherheit zwei MC vorzusehen, die sich durch Parallelrechnung und/oder Plausibilitätsprüfungen

gegenseitig überprüfen. Insbesondere Kostenbetrachtungen führen jedoch zu der Überlegung, bei solchen Steuergeräten lediglich einen einzigen MC zu verwenden.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Steuergerät der eingangs genannten Art dahingehend auszugestalten und weiterzubilden, daß die Zuverlässigkeit der Fehlerdetektion weiter verbessert und die Detektion auf zusätzliche Fehlerarten ausgeweitet wird.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von einem Steuergerät der eingangs genannten Art vor, daß die Überwachungseinheit (CU) erste Mittel zur Messung des Ruhestroms des Mikrocomputers (MC) aufweist und zwischen den ersten Mitteln der CU und dem MC mindestens eine Handshake-Leitung zur Steuerung der Messung des Ruhestroms verläuft, und daß die CU zweite Mittel zur Beaufschlagung des MC mit einem Testdateneingangssignal, zur Verarbeitung des Testdateneingangssignals und zum Vergleich des entsprechenden Testdatenausgangssignals des MC mit dem entsprechenden Testdatenausgangssignal der CU aufweist und zwischen den zweiten Mitteln der CU und dem MC mindestens eine Testdatensignal-Übertragungsleitung verläuft.

Erfindungsgemäß ist erkannt worden, daß die Zuverlässigkeit der Fehlerdetektion erhöht werden kann, indem zwei unterschiedliche, sich gegenseitig ergänzende Testverfahren eingesetzt werden. Auf diese Weise kann auch eine wesentlich größere Anzahl von unterschiedlichen Fehlerarten der Rechenbausteine des MC detektiert werden.

Das erfindungsgemäße Steuergerät kann auch mehrere MCs und mehrere CUs aufweisen. Nachfolgend wird jedoch davon ausgegangen, daß das Steuergerät einen MC und eine CU aufweist. Die CU des erfindungsgemäßen Steuergeräts weist erste Mittel zur Messung des Ruhestroms des MC auf.

Zwischen den ersten Mitteln der CU und dem MC verläuft mindestens eine Handshake-Leitung zur Steuerung der Messung des Ruhestroms. Die Handshake-Leitung kann bspw. als eine bidirektionale Leitung ausgebildet sein.

Die Ruhestrommessung wird nach dem Einschalten des Steuergeräts für eine feste Anzahl (typischerweise 8 bis 16) von ausgewählten Befehlen im Rahmen eines Testprogramms durchgeführt. Für den Mikrocomputer TMS470 werden beispielsweise 14 ausgewählte Befehle abgearbeitet, die einen internen Maschinenzyklus enthalten.

Zur Ergänzung der Ruhestrommessung weist die CU des erfindungsgemäßen Steuergeräts zweite Mittel auf. Zwischen den zweiten Mitteln der CU und dem MC verläuft mindestens eine Testdatensignal-Übertragungsleitung.

Die zweiten Mittel beaufschlagen den MC mit einem Testdateneingangssignal. Der MC berechnet ein Testdatenausgangssignal, das von dem Testdateneingangssignal und den Zuständen im Inneren des MC abhängig ist. Fehlerhafte Zustände führen zu einem veränderten Testdatenausgangssignal des MC.

In den zweiten Mitteln der CU wird auch das Testdateneingangssignal zu einem Testdatenausgangssignal verarbeitet, das als Referenzsignal für die Überprüfung des Testdatenausgangssignals des MC dient. Bei der Berechnung des Testdatenausgangssignal geht die CU von einem fehlerfrei arbeitenden MC aus. Die durchgeführte Berechnung ist vorzugsweise sehr einfach gestaltet. Es wird nicht wie bei Parallelrechnersystemen der Mikrorechner doppelt ausgelegt und von der CU die gleiche Berechnung wie von dem MC ausgeführt. Vielmehr wird so vorgegangen, daß der MC ausgehend von den Eingangsdaten einer vorgegebenen Prüffunktion die Ausgangsdaten berechnet, deren Ergebnisse

von der CU mit dem von ihr berechneten Referenzsignal überprüft werden. Die zur Berechnung der Ausgangsdaten verwendete Prüffunktion ist in der Regel sehr einfach gestaltet, sie erfordert nur eine sehr geringe Rechenzeit. Es können aber auch komplexe Tests und Ergebnisse von den Anwendungsprogrammen in diese Prüffunktion mit einbezogen werden.

Schließlich wird das Testdatenausgangssignal der CU mit dem Testdatenausgangssignal des MC verglichen. Weichen sie voneinander ab oder überschreitet die Abweichung einen vorbestimmten Schwellenwert, erkennt die CU einen Fehler des MC. Das Testergebnis kann mittels einer Anzeigevorrichtung zur Anzeige gebracht werden und/oder es kann vorgesehen sein, daß beim Auftreten eines Fehlers eine Abschaltung des durch das Steuergerät geregelten und/oder gesteuerten Systems vorgesehen ist.

Gemäß einer vorteilhaften Weiterbildung der Erfindung wird vorgeschlagen, daß die ersten Mittel eine IDDQ-Meßschaltung, eine Spannungsversorgung, eine IDDQ-Meßablaufsteuerung (MAS) und eine Steuerung der CU umfassen und daß die Verbindung zwischen den ersten Mitteln und dem MC zwei Handshake-Leitungen, die von der IDDQ-MAS zu dem MC verlaufen, und mindestens eine Spannungsversorgungsleitung, die von der Spannungsversorgung zu dem MC verlaufen, umfaßt, wobei zumindest eine der Spannungsversorgungsleitungen über die IDDQ-Meßschaltung verläuft. Mit IDD wird bei Halbleitern der positive Versorgungsstrom bezeichnet. IDDQ ist eine Bezeichnung des Ruhestroms. Die Handshake-Leitungen sind bspw. als START- und als END-Handshake-Leitungen zum Einleiten bzw. zum Rückmelden des Abschlusses des Funktionstests ausgebildet.

Die Kommunikation zwischen dem MC und der CU zur Messung des Ruhestroms erfolgt über die zwei Handshake-Leitungen.

Die Messung des Ruhestroms des MC durch die CU erfolgt über die separaten Spannungsversorgungsleitungen.

Wie erwähnt, betrifft die Erfindung ein Steuergerät mit einer Überwachungseinheit zum Test des Mikrocomputers des Steuergeräts. Zur Spannungsversorgung des Steuergeräts und damit auch des Mikrocomputers ist eine Spannungsversorgungseinheit vorgesehen. Die Steuereinheit der CU enthält Mittel, die den MC in bestimmte Betriebszustände überführen können. Weiterhin sind in der IDDQ-Meßschaltung Meßmittel vorhanden, die den Strom oder die Spannung im Spannungsversorgungskreis des MC erfassen, woraufhin in Vergleichsmitteln, die ebenfalls in der IDDQ-Meßschaltung vorhanden sind, der erfaßte Strom oder die erfaßte Spannung mit wenigstens einem vorgegebenen Schwellenwert verglichen wird.

Mit der IDDQ-Messung können durch eine einfache Strom- bzw. Spannungsmessung eine Vielzahl von möglichen Fehlern im Rechner erfaßt werden. Dabei kann mit wenigen Testschritten eine hohe Abdeckung der häufigsten Fehler in den Bauteilen eines MC erreicht werden. Solche Fehler können Haftfehler (Stuck-at), Brückenfehler (Bridging) und/oder Unterbrechungsfehler (Stuck-Open) sein.

Die Kombination der Ruhestrommessung mit einem geeigneten anderen Überprüfungsverfahren, insbesondere mit einer Überprüfung der Funktion des MC anhand von Testdatensätzen, ergibt eine insbesondere für sicherheitskritische Anwendungen vorteilhafte breite Fehlerabdeckung bezüglich der wesentlichen Fehler bei Rechnerbausteinen, insbesondere bei CMOS-Prozessoren.

Die oben erwähnte Einsparung des zweiten Prozessors bleibt als wirtschaftlicher Vorteil bei dem erfindungsgemäßen Steuergerät weitgehend erhalten, da die erfindungsgemäße

Ruhestrommessung nur wenig Hardware-Aufwand erfordert.

Die IDDQ-MAS überführt vorgegebene Teile des MC durch eine spezielle Ansteuerung des MC in einen Zustand geringen Stroms. Der Hintergrund dieser Ansteuerung besteht darin, daß im MC meist Bauteile vorhanden sind, die einen relativ hohen Strom benötigen. Da, wie eingangs erwähnt, die Ruhestrommessung im allgemeinen auf Schwankungen des Ruhestroms innerhalb relativ geringer Bandbreiten basiert, stören die Bauteile des MC mit hoher Stromaufnahme die IDDQ-Messung. Insbesondere ist vorgesehen, daß solche Bauteile in den Zustand geringen Stromes überführt werden, auf die sich die IDDQ-Messung nicht bezieht. Solche Bauteile können die MC-Endstufe und/oder eine Eingangsstufe (beispielsweise Analog/Digital-Wandler) sowie Schaltungen zur internen Taktvervielfachung sein. Im einfachsten Fall werden die Bauteile mit hoher Stromaufnahme während des Tests abgeschaltet. Es werden also interne Schaltungsteile und -ausgänge, die hohe Ströme führen, abgeschaltet. Danach kann die Messung des Ruhestroms vorgenommen werden.

Über die oben erwähnte Abschaltung der Bauteile des MC mit hohem Strom hinaus kann auch vorgesehen sein, daß der Kern des MC in einen Zustand geringer Stromaufnahme zu überführen ist. Bei solchen speziell für die Ruhestrommessung ausgelegten MC-Bausteinen ist ein spezieller Betriebszustand, ein sog. IDDQ-Testmode vorgesehen. In diesem Betriebszustand werden alle rechnerinternen Ströme ausgeschaltet, d. h. der Strom im MC-Kern wird minimiert. Das IDDQ-Design ist derart, daß sich Standardfehler im MC-Kern in einer Erhöhung des Ruhestroms bemerkbar machen. So äußern sich beispielsweise Kurzschluß- bzw. Haftfehler (Kurzschluß nach Masse oder Versorgungsspannung) sofort in einer Erhöhung des Ruhestromes. Es ist hierbei nicht notwendig, die Auswirkung eines solchen Fehlers bis auf die Ausgänge des MC

weiterzuleiten (zu propagieren). Die erhöhte Stromaufnahme ist der sofortige Fehlerindikator.

Neben dem oben beschriebenen IDDQ-Testmode kann vorgesehen sein, daß nur die Bauteile des MC mit hohem Strom abgeschaltet werden und der MC auf einen Befehl hin in einen definierten Zustand mit niedrigem Strom übergeht. Dabei braucht der MC-Kern nicht speziell für den IDDQ-Testmode ausgelegt zu sein. Dies wird als Power-Down-Mode bezeichnet.

Der Power-Down-Mode wird eingeleitet, indem rechnerinterne Teile wie Register und Speicher mit bestimmten Mustern geladen werden und die oben erwähnten Rechnerbauteile in den Zustand geringer Stromaufnahme überführt werden, bspw. durch Ausführung eines bestimmten Rechnerbefehls. Ist dieser Zustand erreicht, so kann wahlweise ein Zeittaktgeber ausgeschaltet bzw. abgetrennt werden. Anschließend wird der Ruhestrom oder ein entsprechender Spannungswert gemessen und mit einem Schwellenwert verglichen, der dem oben eingestellten Betriebszustand (Power-Down-Zustand) des MC-Kerns entspricht. Sind im Rechner bestimmte Fehler vorhanden (Haftfehler, Brückenfehler, Unterbrechungen), so führt dies meist zu einer Erhöhung des Ruhestroms beziehungsweise des durch den Ruhestrom verursachten Spannungsabfalls.

Nach einem solchen Testschritt können weitere Testschritte folgen, indem zunächst der Power-Down-Mode durch Anlegen von bestimmten Signalpegeln an bestimmte Anschlüsse des MC verlassen wird. Durch ein erneutes Starten bzw. Zuschalten des Zeittaktgebers werden die rechnerinternen Teile wie Register und Speicher mit weiteren Mustern geladen und es werden wiederum die oben erwähnten Bauteile in den Zustand geringen Stroms überführt, bspw. durch Ausführen eines bestimmten Rechnerbefehls (Power-Down-Befehl). Daran

schließt sich wiederum die oben beschriebene Messung des Ruhestromes an. Durch mehrere solcher hintereinander ausgeführter Messungen des Power-Down-Stroms gelangt man zu einer immer vollständigeren Fehlererfassung von Registern, Speichern und Teilen des Rechnerkerns.

Die einzelnen Testschritte werden je nach Rechnertyp und Ausführung der Schaltung durch eine Wiederfreigabe des Zeittaktgebers, einer Reset-Auslösung oder einer Auslösung eines externen Interrupts beendet. Nach dem letzten Testschritt wird der MC wieder in seinen normalen Betriebsmodus betrieben (Normalbetrieb).

Neben der oben beschriebenen Ruhestrommessung im Power-Down-Mode ist auch erfindungsgemäß eine Messung des Ruhestroms in dem erwähnten IDDQ-Testmode vorgesehen, sofern der zu testende Rechner dafür ausgelegt ist. Der Eintritt des IDDQ-Testmodes wird bspw. durch Verändern des Signalpegels an einem Anschluß des MC eingeleitet. Auch hierbei werden vor Eintritt in den IDDQ-Testmode Register und Speicher mit bestimmten Mustern geladen. Mit Eintritt des IDDQ-Testmodes werden die Rechnerteile mit hoher Stromaufnahme abgeschaltet. Darüber hinaus kann der Rechnerkern durch Anhalten bzw. Abkoppeln des Zeittaktes während der Ausführung eines Befehls in einem für diesen Befehl typischen Zustand gehalten werden. Diese Befehle sind derart ausgewählt, daß sie die Zustände der internen Schaltungsknoten des Rechnerkerns so einstellen, daß möglichst viele Fehler über die Ruhestrommessung detektiert werden können.

Der Handshake für die Ruhestrommessung erfolgt in mehreren Schritten:

S1: Der MC setzt das START-Signal auf HIGH. Damit weiß die CU, daß eine IDDQ-Messung beginnt.

S2: Wahlweise kann der MC das Anhalten des Zeittakts (Master Clock, MCLK) vorbereiten, indem er durch einen internen Befehl ein Signal PREP auf LOW setzt.

S3: Der MC dekodiert den genau definierten Zeitpunkt innerhalb des nächsten geeigneten Befehls für den IDDQ-Test und setzt ein Signal DEKOD ebenfalls auf LOW. Jetzt wird die MCLK gleich LOW und der Digitalteil des MC ist für die IDDQ-Messung auf statischen Betrieb eingestellt.

S4: Die CU führt die IDDQ-Messung durch.

S5: Die CU gibt die Pegelfolge LOW-HIGH-LOW am Signal END aus und aktiviert damit wieder die MCLK.

S6: Der MC wird wieder aktiv und bestätigt das Ende der Messung durch Setzen des START-Signals auf LOW. Der MC setzt das Programm fort und bereitet die nächste IDDQ-Messung vor oder beendet die IDDQ-Messungen, wenn alle Messungen durchgeführt sind.

Vorzugsweise verlaufen zwischen der Spannungsversorgung und dem MC zwei Spannungsversorgungsleitungen, wobei eine Spannungsversorgungsleitung über die IDDQ-Meßschaltung verläuft. Über die Spannungsversorgungsleitung, die über die IDDQ-Meßschaltung verläuft, wird der Ruhestrom des MC gemessen.

Gemäß einer anderen vorteilhaften Weiterbildung des erfindungsgemäßen Steuergeräts wird vorgeschlagen, daß die ersten Mittel eine IDDQ-Meßschaltung, eine Spannungsversorgung, eine IDDQ-Meßablaufsteuerung (MAS) und eine Steuerung der CU umfassen und daß die Verbindung zwischen den ersten Mitteln und dem MC vier Handshake-Leitungen die von der IDDQ-MAS zu dem MC verlaufen, und mindestens eine Spannungsversorgungsleitung, die von der Spannungsversorgung zu dem MC verlaufen, umfaßt, wobei zumindest eine der Spannungsversorgungsleitungen über die IDDQ-Meßschaltung verläuft. Bei vier Handshake-Leitungen

können zusätzlich zu den Leitungen START, END bei zwei Handshake-Leitungen noch eine Zeittakt (CLK)-Leitung und eine Leitung für eine Power-Down (PWRDN)-Ansteuerung für den MC vorgesehen werden. Bei dieser Ausführungsform des Steuergeräts genügt eine gemeinsame Spannungsversorgungsleitung zum Prozessor, in der der Ruhestrom gemessen wird. Das Anhalten des Zeittaktgebers erfolgt dann in der CU. Die Ansteuerung von Spannungsversorgungsschaltern für Analog- und IO-Schaltungen im MC erfolgt durch die PWRDN-Leitung aus der CU. Somit fließt im Meßfall nur der Ruhestrom des Digitalteils des MC über die gemeinsame Spannungsversorgungsleitung.

Vorteilhafterweise weisen die ersten Mittel eine Initialisierungsschaltung auf, die nach dem Einschalten des Steuergeräts von der Spannungsversorgung ein Initialisierungssignal erhält und danach zur Freigabe der IDDQ-Messung ein Freigabe-Signal an die IDDQ-MAS sendet. Der erfolgreiche Abschluß der IDDQ-Messung wird durch ein weiteres Signal an die Steuerung der CU signalisiert. Die CU schaltet daraufhin den Testablauf weiter, indem die Initialisierungsschaltung über ein weiteres Signal den Testdatensignalgenerator freigibt.

Gemäß einer vorteilhaften Ausführungsform der vorliegenden Erfindung weisen die zweiten Mittel einen Testdatensignalgenerator zur Beaufschlagung des MC mit einem Testdateneingangssignal, einen Antwortgenerator zur Verarbeitung des Testdateneingangssignals und zur Bildung eines entsprechenden Testdatenausgangssignals, ein Testdatenregister zum Senden und Empfangen der Testdaten und einen Vergleicher zum Vergleich des Testdatenausgangssignals des MC mit dem Testdatenausgangssignal der CU umfassen und daß die Verbindung zwischen den zweiten Mitteln und dem MC

mindestens eine Testdatenübertragungsleitung umfasst, die zwischen dem Testdatenregister und dem MC verlaufen. Vorteilhafterweise verlaufen zwichen dem Testdatenregister und dem MC zwei Testdatenübertragungsleitungen.

Auch der Testdatensignalgenerator wird durch die Initialisierungsschaltung nach dem Einschalten des Steuergeräts aktiviert. Im Testdatensignalgenerator werden die Testdaten für den MC in einer quasi-zufälligen Reihenfolge durch ein rückgekoppeltes Schieberegister generiert. Zu jedem Testdateneingangssignal wird in dem Antwortgenerator mit Hilfe des Reed-Muller-Codes die Bitfolge für das Testdatenausgangssignal (das sog. Referenzsignal) gebildet. Dieser Code wird angewendet, um einen größtmöglichen Abstand im Zahlenraum der Testdatenausgangssignale (Hamming-Distanz) zu erhalten. Im Vergleicher wird dann das theoretisch berechnete Testdatenausgangssignal aus dem Antwortgenerator der CU mit dem tatsächlichen Testdatenausgangssignal des MC aus dem Testdatenregister verglichen.

Die zweiten Mittel weisen vorzugsweise einen Triggergenerator auf, der den Zeitpunkt ermittelt, zu dem das Testdatenausgangssignal des MC bei fehlerfreiem MC an dem Vergleicher anliegt. Der Triggergenerator gibt den Zeitpunkt des Vergleichs des ermittelten Testdatenausgangssignals des MC mit der tatsächlichen Antwort des CU vor. Dadurch wird sichergestellt, daß die Zeitscheiben in dem MC richtig ablaufen. Der Vergleicher prüft das Testdatenausgangssignal nicht nur auf den richtigen Datenwert hin, sondern auch, ob das Testdatenausgangssignal innerhalb eines bestimmten Zeitfensters übertragen wird.

Vorteilhafterweise weisen die zweiten Mittel einen Fehlerzähler auf, der hoch- oder runterzählt, falls das

Testdatenausgangssignal des MC nicht mit dem Testdatenausgangssignal der CU übereinstimmt und/oder falls das Testdatenausgangssignal des MC zu einem anderen als zu dem von dem Triggergenerator ermittelten Zeitpunkt an dem Vergleicher anliegt. Der Vergleicher bewirkt durch einen Zählimpuls das Hoch- oder Runterzählen des Fehlerzählers. Sind Wert und Zeitpunkt des Testdatenausgangssignals richtig, wird der Fehlerzähler bspw. dekrementiert. Unterschreitet der Fehlerzähler einen vorgebbaren Wert, wird über ein Signalinterface bspw. eine externe Warnlampe an- oder abgeschaltet und ein Relais zum Manipulieren der sicherheitskritischen Anwendung freigegeben.

Die Manipulation der zu steuernden Anwendung wird sich in der Regel auf ein Abschalten der Anwendung beschränken. Bei besonderen Anwendung kann es jedoch sinnvoll sein, daß der Fehlerzähler mehrere Ansprechschwellen hat, deren Überschreiten jeweils eine unterschiedliche Reaktion zur Folge hat. Dadurch kann ein sofortiges Abschalten der Anwendung bei einer einmaligen Störung verhindert und eine Überprüfung des Abschaltpfades durch den Rechner ermöglicht werden.

Wird ein Testdateneingangssignal zum falschen Zeitpunkt oder mit einem falschen Wert durch den MC beantwortet, wird der MC mit demselben Testdateneingangssignal nochmals beaufschlagt bis der Zeipunkt und der Wert des Testdatenausgangssignals richtig sind. Tritt dies innerhalb einer vordefinierten Zeit nicht ein, schaltet die CU das Steuergerät bzw. die Anwendung ab und kann auch durch richtige Antworten nicht mehr aktiviert werden.

Die zweiten Mittel weisen vorzugsweise eine Initialisierungsschaltung auf, die nach dem Einschalten des Steuergeräts von der Spannungsversorgung ein Initialisierungssignal erhält, danach die CU mit dem MC

synchronisiert und danach den Testdatensignalgenerator und den Fehlerzähler aktiviert. Die CU wird mit dem MC synchronisiert, indem die CU auf die ersten Datenübertragung des MC wartet.

Eine weitere Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren zum Überprüfen eines Mikrocomputers der eingangs genannten Art dahingehend auszugestalten und weiterzubilden, daß die Zuverlässigkeit der Fehlerdetektion weiter verbessert und die Detektion auf zusätzliche Fehlerarten ausgeweitet wird.

Zur Lösung dieser Aufgabe schlägt die Erfindung ausgehend von dem Verfahren der eingangs genannten Art vor, dass die CU des Steuergeräts

- eine Messung des Ruhestroms des MC durchführt und
- den MC mit einem Testdateneingangssignal beaufschlagt
- ein erstes Testdatenausgangssignal bestimmt und
- ein zweites Testdatenausgangssignal des MC mit dem ersten Testdatenausgangssignal der CU vergleicht.

Vorteilhafterweise ist die Ruhestrommessung als eine IDDQ-Messung ausgebildet. Vorzugsweise wird die IDDQ-Messung nach dem Einschalten des Steuergerätes nach der Freigabe durch ein Freigabesignal durchgeführt.

Gemäß einer vorteilhaften Weiterbildung des erfindungsgemäßen Verfahrens wird der Vergleich des zweiten Testdatenausgangssignals des MC mit dem ersten Testdatenausgangssignal der CU während des Betriebs des Steuergeräts durchgeführt. Das hat den Vorteil, daß das Steuergerät nicht abgeschaltet werden muß, um die Funktion des Mikrocomputers überprüfen zu können. Vielmehr können während des Betriebs des Steuergeräts nicht zur Steuerung der Anwendung genutzte Rechenkapazitäten des MC zur Überprüfung des MC genutzt werden.

Vorzugsweise wird während des Betriebs des Steuergeräts in regelmäßigen Abständen einmalig ein falsches Testdatenausgangssignal an die CU ausgegeben, um die Funktion des Abschaltpfades zu überprüfen.

Eine weitere vorteilhafte Ausgestaltung der Erfindung geht davon aus, daß während der IDDQ-Messung und/oder während des Vergleichs des zweiten Testdatenausgangssignals des MC mit dem ersten Testdatenausgangssignal der CU ein Zeittaktgeber durch den MC angehalten wird. Der Zeittaktgeber ist in der Steuerung der CU vorgesehen. Abhängig von den Ausgangssignalen dieses Zeittaktgebers werden insbesondere die rechnerinternen Vorgänge gesteuert. Bei dem beschriebenen IDDQ-Testmode ist vorgesehen, daß dieser Zeittaktgeber aus- oder abgeschaltet bzw. von dem MC abgetrennt wird. Dies kann auch beim Power-Down-Mode realisiert sein, wenn ein besonders niedriger Ruhestrom erzielt werden soll. Diese Aus- oder Abschaltung bzw. das Abtrennen des Zeittaktgebers geschieht insbesondere zu Beginn einer jeden Ruhestrommessung.

Vorzugsweise wird das Testdateneingangssignal der CU von einem Testdatensignalgenerator durch ein rückgekoppeltes Schieberegister generiert. Vorteilhafterweise wird das Testdatenausgangssignal der CU von einem Antwortgenerator mit Hilfe des Reed-Muller-Codes generiert.

Das erfindungsgemäße Steuergerät kann mittels zweier unterschiedlicher Testabläufe überprüft werden. Ein sog. Startup-Test wird unmittelbar nach dem Einschalten des Steuergeräts und vor dem Betrieb des Steuergeräts zur Steuerung oder Regelung der sicherheitskritischen Anwendung durchgeführt. Ein sog. Online-Test wird nach dem Startup-Test während des Betriebs des Steuergeräts von Zeit zu Zeit durchgeführt.

Der Startup-Test ist in zwei Testabschnitte unterteilt, den sog. Prozessorinitialisierungs-Abschnitt (Proz-Init) und den anschließenden sog. Betriebssysteminitialisierungs-Abschnitt (BS-Init). Der Proz-Init-Abschnitt umfaßt einen Befehls- und Core-Test, einen RAM/ROM-Test und einen IDDQ-Test. Der BS-Init-Abschnitt umfaßt eine Startup-Regelung und einen Test der CU. Bei der Startup-Regelung werden dem Steuergerät verschiedene Eingangswerte vorgespielt (bspw. ein bestimmter Drehzahlverlauf der Räder eines Fahrzeugs, wie er typischerweise am Eingang eines ABS-Steuerungsgeräts des Fahrzeugs auftreten kann). Das Steuergerät führt aufgrund der Eingangswerte eine Regelung bzw. Steuerung der Anwendung durch. Das Ergebnis dieser simulierten Regelung bzw. Steuerung wird mit entsprechenden Sollwerten verglichen. Bei dem Test der CU wird ein defekter MC simuliert und die Reaktion der CU auf den Defekt überprüft.

Der Online-Test weist einen Befehls- und Core-Test, einen RAM/ROM-Test, einen Test der CU, und einen Replications-Test auf. Bei dem Replications-Test werden für bestimmte sicherheitskritische Variable doppelte Speicherplätze vorgesehen und bestimmte sicherheitskritische Berechnungen doppelt ausgeführt. Die Inhalte der doppelten Speicherplätze und die Ergebnisse der doppelten Berechnungen werden miteinander verglichen. Die redundante Speicherung und die redundante Berechnung erfolgt durch den einen Prozessor des Steuergeräts. Der Online-Test weist darüber hinaus eine Plausibilitätsüberwachung auf, bei der die von dem MC ermittelten Steuerungs- bzw. Regelungssignale auf Plausibilität überprüft werden. Bei einem ABS-Steuergerät kann bspw. überprüft werden, ob die Geschwindigkeit, die Beschleunigung oder die Verzögerung innerhalb bestimmter Grenzen liegt. Außerdem müssen die Werte der einzelnen Räder des Fahrzeugs in einer bestimmten Relation zueinander stehen, was ebenfalls überprüft werden kann. Der Online-Test weist schließlich noch einen

Betriebssystem-Test und einen Test der übrigen Überwachungseinheiten des Steuergeräts auf.

Ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung wird im folgenden anhand der Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein schematisches Übersichtsblockschaltbild eines erfindungsgemäßen Steuergeräts;

Fig. 2 ein detailliertes Übersichtsblockschaltbild des Steuergeräts aus Fig. 1;

Fig. 3 eine Schaltungsanordnung für eine Ruhestrommessung mit Zweidraht-Handshake; und

Fig. 4 Zeitdiagramm der Meßablaufsteuerung für die Ruhestrommessung aus Fig. 3.

In Fig. 1 ist ein schematisches Übersichtsblockschaltbild eines erfindungsgemäßen Steuergeräts dargestellt. Das erfindungsgemäße Steuergerät ist in seiner Gesamtheit mit dem Bezugszeichen 1 gekennzeichnet. Das Steuergerät 1 dient zur Steuerung sicherheitskritischer Anwendungen, bspw. für Antiblockiersysteme, für Antriebsschlupfregelsysteme und/oder für Fahrdynamikregelsysteme. Das Steuergerät 1 weist einen Mikrocomputer MC, eine Überwachungseinheit (CU, Check Unit) und Peripherieschaltungen (IO, Input/Output). Der Mikrocomputer MC, die Überwachungseinheit CU und die Peripherieschaltungen IO sind über einen seriellen synchronen Datenbus 2 in Serie geschaltet. Der Mikrocomputer MC sendet über seine Datenausgabeleitung MC_Dout die Datenausgangssignale über den Datenbus 2 an die Busteilnehmer und empfängt gleichzeitig die Dateneingangssignale über seine Dateneingabeleitung MC_Din. Mit dem Signal SAM (Sample) speichern die Busteilnehmer die

in ihren Speicherregistern angekommenen Daten ab.

Zwischen dem Mikrocomputer MC und der Überwachungseinheit CU bestehen weitere Verbindungsleitungen, nämlich eine gemeinsame Versorgungsleitung VDD oder wahlweise mehrere Versorgungsleitungen VDD für eine digitale und analoge Versorgung des Mikrocomputers MC. Schließlich verlaufen zwischen dem Mikrocomputer MC und der Überwachungseinheit CU IDDQ-Handshake-Leitungen IDDQ-HDSHK, die zur Steuerung der Ruhestrommessung (IDDQ-Messung) des Mikrocomputers MC dienen. Aus der Überwachungseinheit CU führen sogenannte Abschaltpfade 3 zu externen Warnlampen und/oder Relais zum Manipulieren der zu steuerenden sicherheitskritischen Anwendungen, je nachdem, ob die Überwachungseinheit CU einen Fehler des Mikrocomputers MC detektiert oder nicht. Die Peripherieschaltungen IO weisen Verbindungsleitungen 4 zu der zu steuernden sicherheitskritischen Anwendung 5 auf.

Nach dem Einschalten des Steuergeräts 1 wird zur Funktionsüberprüfung des Mikrocomputers MC eine Ruhestrommessung durchgeführt. Während des Betriebs des Steuergeräts 1 wird die Funktion des Mikrocomputers MC überprüft, indem er regelmäßig mit Testdatensätzen beaufschlagt wird und das entsprechende zweite Testdatenausgangssignal des MC mit einem von der Überwachungseinheit CU berechneten fehlerfreien ersten Testdatenausgangssignal verglichen wird.

In Fig. 2 ist ein detailliertes Übersichtsblockschaltbild des Steuergeräts 1 aus Fig. 1 dargestellt. Die Überwachungseinheit CU umfasst eine Steuerung 6 der Überwachungseinheit CU, eine Messablaufsteuerung 7 für die IDDQ-Messung, eine IDDQ-Messschaltung 8 und eine Spannungversorgung 9.

Die Steuerung 6 der Überwachungseinheit CU umfasst einen Testdatensignalgenerator 10, einen Antwortgenerator 11 und einen Vergleicher 12. Mit Hilfe des Testdatensignalgenerators 10 wird der Mikrocomputer MC mit einem Testdateneingangssignal beaufschlagt und ermittelt in Abhängigkeit von dem Testdateneingangssignal und von seinen internen Zuständen ein zweites Testdatenausgangssignal. Der Antwortgenerator 11 verarbeitet dasselbe Testdateneingangssignal und bildet ein entsprechendes erstes Testdatenausgangssignal. In dem Vergleicher 12 wird das erste Testdatenausgangssignal der Überwachungseinheit CU mit dem zweiten Testdatenausgangssignal des Mikrocomputers MC verglichen. Ein Triggergenerator 13 ermittelt den Zeitpunkt, zu dem das zweite Testdatenausgangssignal des Mikrocomputers MC bei fehlerfrei arbeitendem Mikrocomputer MC an dem Vergleicher 12 anliegt.

Die Steuerung 6 der Überwachungseinheit CU weist darüber hinaus einen Fehlerzähler 14 auf, der einen Fehler zählt, falls das zweite Testdatenausgangssignal des Mikrocomputers MC nicht mit dem ersten Testdatenausgangssignal der Überwachungseinheit CU übereinstimmt und/oder falls das zweite Testdatenausgangssignal des Mikrocomputers MC zu einem anderen als zu dem von dem Triggergenerator 13 ermittelten Zeitpunkt an dem Vergleicher 12 anliegt.

Des weiteren weist die Steuerung 6 der Überwachungseinheit CU ein Testdatenregister 17 auf, das zum Senden und Empfangen der Testdaten dient.

Die Steuerung 6 der Überwachungseinheit CU weist schließlich auch eine Initialisierungsschaltung 15 auf, die nach dem Einschalten des Steuergeräts 1 von der Spannungsversorgung 9 ein Initialisierungssignal RST erhält, und danach die Überwachungseinheit CU mit dem

Mikrocomputer MC synchronisiert, indem sie auf die erste Datenübertragung des MC wartet. Danach aktiviert die Initialisierungsschaltung 15 den Testdatensignalgenerator 10 und den Fehlerzähler 14.

In dem Testdatensignalgenerator 10 werden die Testdateneingangssignale für den Mikrocomputer MC in einer quasi-zufälligen Reihenfolge durch ein rückgekoppeltes Schieberegister generiert. Zu jedem Testdateneingangssignal wird in dem Antwortgenerator 11 mit Hilfe des "Reed-Muller-Codes" die Bit-Folge für das entsprechende erste Testdatenausgangssignal gebildet. Dieser Code wird angewendet, um einen größtmöglichen Abstand im Zahlenraum der Testdatenausgangssignale (Hamming-Distanz) zu erhalten. In dem Vergleicher 12 wird dann das in dem Antwortgenerator 11 ermittelte erste Testdatenausgangssignal mit dem tatsächlichen zweiten Testdatenausgangssignal des Mikrocomputers MC verglichen.

Der Zeitpunkt des Vergleichs wird durch den Triggergenerator 13 vorgegeben. Dies stellt sicher, dass die Zeitscheiben in dem Mikrocomputer MC richtig ablaufen. Der Vergleicher 12 prüft das zweite Testdatenausgangssignal des MC nicht nur auf den richtigen Datenwert hin, sondern auch, ob das Testdatenausgangssignal innerhalb eines bestimmten Zeitfensters übertragen wird. Sind Wert und Zeitpunkt des zweiten Testdatenausgangssignals des MC richtig, wird der Fehlerzähler 14 dekrementiert und über ein Signal-Interface 16 die zu steuernde sicherheitskritische Anwendung im aktiven Zustand gehalten, indem externe Warnlampen ausgeschaltet und Relais zum Ansteuern der Anwendung 5 aktiviert werden.

In jedem auf diesen ersten Zyklus folgenden Zyklus muss der Zeitpunkt und der Wert des zweiten Testdatenausgangssignals des MC richtig sein, um ein sofortiges Ansprechen des

Fehlerzählers 14 zu verhindern. Der Fehlerzähler 14 hat mehrere Ansprechschwellen, um ein Abschalten des Steuergeräts 1 bzw. der Anwendung 5 bei einer einmaligen Störung zu verhindern und um eine Prüfung des Abschaltpfades durch den Mikrocomputer MC zu ermöglichen. Die erste Stufe sperrt die Ventilendstufen durch das Signal EN und schaltet die Spannungsversorgung der Ventile über das Ventilrelais VRA aus. Die Anzeige der Warnlampen SILA wird um einen Zyklus verzögert, damit beim Testen des Abschaltpfades keine Anzeige erfolgt.

Wird ein Testdateneingangssignal zum falschen Zeitpunkt oder mit einem falschen Wert beantwortet, wird der Mikrocomputer MC mit demselben Testdateneingangssignal nochmals beaufschlagt, bis der Zeitpunkt und der Wert richtig sind. Tritt dies innerhalb einer vordefinierten Zeit nicht ein, schaltet die Überwachungseinheit CU das Steuergerät 1 ab und kann auch durch richtige Antworten nicht mehr aktiviert werden.

Die Ruhestrommessung wird nach dem Einschalten des Steuergeräts 1 für eine feste Anzahl (typischerweise 8 bis 16) von Zeitpunkten eines Testprogramms durchgeführt. Die Kommunikation zwischen Mikrocomputer MC und Überwachungseinheit CU zur Ruhestrommessung erfolgt über die zwei Handshake-Leitungen START und END. Während der Ruhestrommessung hält der Mikrocomputer MC den Zeittaktgeber CLK an. Zwischen der Überwachungseinheit CU und dem Mikrocomputer MC sind zwei separate Spannungsversorgungsleitungen, VDD_digital zur Versorgung des Digitalteils des Mikrocomputers MC und VDD_analog zur Versorgung des Analogteils des Mikrocomputers MC. Der Ruhestrom wird in der Spannungsversorgungsleitung VDD_digital gemessen.

Die Freigabe der Ruhestrommessung erfolgt nach dem

Einschalten der Versorgungsspannung durch das Signal IDDQ_EN der Steuerung 6 der Überwachungseinheit CU. Der erfolgreiche Abschluss der Ruhestrommessung wird durch das Signal IDDQ_FIN an die Steuerung 6 der Überwachungseinheit CU signalisiert. Die Überwachungseinheit CU schaltet dann den Testablauf weiter, indem die Initialisierungsschaltung 15 über ein Signal IDDQ_OK den Testdatensignalgenerator 10 freigibt.

In Fig. 3 ist eine Schaltungsanordnung für die Ruhestrommessung mit einem Zweidraht-Handshake dargestellt. In Fig. 4 ist das Zeitdiagramm der Messablaufsteuerung 7 für die Ruhestrommessung aus Fig. 3 dargestellt. Nach dem Einschalten des Steuergeräts 1 startet der Mikrocomputer MC seinen Selbsttest. Ein Teil dieses Selbsttests ist die Ruhestrommessung. Erreicht der Ablauf im Mikrocomputer MC den Ruhestromtest, wird das Signal START aktiviert. Zum Zeitpunkt T1 wird die Ruhestrommessung durch das Signal M_Act aktiviert. Der Ausgang des Vergleichers 12 für die Ruhestrommessung wird nach der Zeit T2 ausgewertet. Ist der Wert in Ordnung, wird der Mikrocomputer MC durch das END-Signal wieder aktiviert. Liegt der Wert außerhalb eines Grenzwertes, wird die Messung wiederholt. Die Anzahl der Wiederholungen ist vorgegeben. Führt auch die Wiederholung der Messung zu keiner richtigen Antwort, wird die Messung abgebrochen und die Überwachungseinheit CU schaltet den Mikrocomputer MC nicht mehr ein, sondern bleibt in einem Fail-safe-Modus. Wenn alle Ruhestrommessungen abgeschlossen sind, wird das Signal IDDQ_FIN auf HIGH gesetzt. Die Steuerung 6 der Überwachungseinheit CU nimmt daraufhin das Signal IDDQ_EN von HIGH auf LOW zurück.

06.08.1998
Robert Bosch GmbH , 70469 Stuttgart

Patentansprüche

1. Steuergerät (1) zur Steuerung sicherheitskritischer Anwendungen (5) mit einem Mikrocomputer (MC), einer Überwachungseinheit (Check Unit, CU) und Peripherieschaltungen (Input Output, IO), dadurch gekennzeichnet, daß die Überwachungseinheit (CU) erste Mittel zur Messung des Ruhestroms des Mikrocomputers (MC) aufweist und zwischen den ersten Mitteln der CU und dem MC mindestens eine Ruhestrom-Handshake-Leitung (IDDQ-HDSHK) zur Steuerung der Messung des Ruhestroms verläuft, und daß die CU zweite Mittel zur Beaufschlagung des MC mit einem Testdateneingangssignal, zur Verarbeitung des Testdateneingangssignals und zum Vergleich des entsprechenden Testdatenausgangssignals des MC mit dem entsprechenden Testdatenausgangssignal der CU aufweist und zwischen den zweiten Mitteln der CU und dem MC mindestens eine Testdatensignal-Übertragungsleitung verläuft.

2. Steuergerät (1) nach Anspruch 1, dadurch gekennzeichnet, daß die ersten Mittel eine IDDQ-Meßschaltung (8), eine Spannungsversorgung (9), eine IDDQ-Meßablaufsteuerung (MAS) (7) und eine Steuerung (6) der CU umfassen und daß die Verbindung zwischen den ersten Mitteln und dem MC zwei Handshake-Leitungen (START, END), die von der IDDQ-MAS zu dem MC verlaufen, und mindestens eine Spannungsversorgungsleitung (VDD), die von der Spannungsversorgung (9) zu dem MC verlaufen, umfaßt, wobei zumindest eine der Spannungsversorgungsleitungen (VDD) über

die IDDQ-Meßschaltung (8) verläuft.

3. Steuergerät (1) nach Anspruch 2, dadurch gekennzeichnet, daß zwischen der Spannungsversorgung (9) und dem MC zwei Spannungsversorgungsleitungen (VDD_analog, VDD_digital) verlaufen, wobei eine Spannungsversorgungsleitung (VDD_digital) über die IDDQ-Meßschaltung (8) verläuft.

4. Steuergerät (1) nach Anspruch 1, dadurch gekennzeichnet, daß die ersten Mittel eine IDDQ-Meßschaltung (8), eine Spannungsversorgung (9), eine IDDQ-Meßablaufsteuerung (MAS) (7) und eine Steuerung (6) der CU umfassen und daß die Verbindung zwischen den ersten Mitteln und dem MC vier Handshake-Leitungen (START, END, CLK, PWR_DN), die von der IDDQ-MAS (7) zu dem MC verlaufen, und mindestens eine Spannungsversorgungsleitung (VDD), die von der Spannungsversorgung (9) zu dem MC verlaufen, umfaßt, wobei zumindest eine der Spannungsversorgungsleitungen (VDD) über die IDDQ-Meßschaltung (8) verläuft.

5. Steuergerät (1) nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, daß die ersten Mittel eine Initialisierungsschaltung (15) aufweisen, die nach dem Einschalten des Steuergeräts (1) von der Spannungsversorgung (9) ein Initialisierungssignal (RST) erhält und danach zur Freigabe der IDDQ-Messung ein Freigabe-Signal (IDDQ_EN) an die IDDQ-MAS (7) sendet.

6. Steuergerät (1) nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die zweiten Mittel einen Testdatensignalgenerator (10) zur Beaufschlagung des MC mit einem Testdateneingangssignal, einen Antwortgenerator (11) zur Verarbeitung des Testdateneingangssignals und zur Bildung eines entsprechenden Testdatenausgangssignals, ein Testdatenregister (17) zum Senden und Empfangen der

Testdaten und einen Vergleicher (12) zum Vergleich des Testdatenausgangssignals des MC mit dem Testdatenausgangssignal der CU umfassen und daß die Verbindung zwischen den zweiten Mitteln und dem MC mindestens eine Testdatenübertragungsleitung umfasst, die zwischen dem Testdatenregister (17) und dem MC verläuft.

7. Steuergerät (1) nach Anspruch 6, dadurch gekennzeichnet, daß die Verbindung zwischen den zweiten Mitteln und dem MC zwei Testdatenübertragungsleitungen (CU_Dout, CU_Din) umfasst.

8. Steuergerät (1) nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß die zweiten Mittel einen Triggergenerator (13) aufweisen, der den Zeitpunkt ermittelt, zu dem das Testdatenausgangssignal des MC bei fehlerfreiem MC an dem Vergleicher (12) anliegt.

9. Steuergerät (1) nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, daß die zweiten Mittel einen Fehlerzähler (14) aufweisen, der einen Fehler zählt, falls das Testdatenausgangssignal des MC nicht mit dem Testdatenausgangssignal der CU übereinstimmt und/oder falls das Testdatenausgangssignal des MC zu einem anderen als zu dem von dem Triggergenerator (13) ermittelten Zeitpunkt an dem Vergleicher (12) anliegt.

10. Steuergerät (1) nach Anspruch 9, dadurch gekennzeichnet, daß der Fehlerzähler (14) mehrere Ansprechschwellen hat, deren Überschreiten jeweils eine unterschiedliche Reaktionen zur Folge hat.

11. Steuergerät (1) nach einem der Ansprüche 6 bis 10, dadurch gekennzeichnet, daß die zweiten Mittel eine Initialisierungsschaltung (15) aufweisen, die nach dem Einschalten des Steuergeräts (1) von der

Spannungsversorgung (9) ein Initialisierungssignal (RST) erhält, danach die CU mit dem MC synchronisiert und danach den Testdatensignalgenerator (10) und den Fehlerzähler (14) aktiviert.

12. Verfahren zum Überprüfen eines Mikrocomputers (MC) eines Steuergeräts (1) zur Steuerung sicherheitskritischer Anwendungen, das den Mikrocomputer (MC), eine Überwachungseinheit (Check Unit, CU) und Peripherieschaltungen (Input Output, IO) aufweist, gekennzeichnet durch

- eine Messung des Ruhestroms des MC und
- eine Beaufschlagung des MC mit einem Testdateneingangssignal,
- ein Bestimmen eines ersten Testdatenausgangssignals und
- einen Vergleich eines zweiten Testdatenausgangssignals des MC mit dem ersten Testdatenausgangssignal der CU.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß die Ruhestrommessung als eine IDDQ-Messung ausgebildet ist.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, daß die IDDQ-Messung nach dem Einschalten des Steuergerätes (1) nach der Freigabe durch ein Freigabesignal (IDDQ_EN) durchgeführt wird.

15. Verfahren nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß der Vergleich des zweiten Testdatenausgangssignals des MC mit dem ersten Testdatenausgangssignal der CU während des Betriebs des Steuergeräts (1) durchgeführt wird.

16. Verfahren nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, daß während der IDDQ-Messung und/oder

während des Vergleichs des zweiten Testdatenausgangssignals des MC mit dem ersten Testdatenausgangssignal der CU ein Zeittaktgeber (Clock, CLK) durch den MC angehalten wird.

17. Verfahren nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, daß das Testdateneingangssignal der CU von einem Testdatensignalgenerator (10) durch ein rückgekoppeltes Schieberegister generiert wird.

18. Verfahren nach Anspruch 17, dadurch gekennzeichnet, daß das Testdatenausgangssignal der CU von einem Antwortgenerator (11) mit Hilfe des Reed-Muller-Codes generiert wird.

06.08.1998
Robert Bosch GmbH , 70469 Stuttgart

Testverfahren und Schaltungsanordnung für Steuergeräte

Zusammenfassung

Die Erfindung betrifft ein Steuergerät (1) zur Steuerung sicherheitskritischer Anwendungen (5) mit einem Mikrocomputer (MC), einer Überwachungseinheit (CU, Check Unit) und Peripherieschaltungen (IO, Input/Output). Um bei derartigen Steuergeräten die Zuverlässigkeit der Fehlerdetektion weiter zu verbessern und die Detektion auf zusätzliche Fehlerarten auszuweiten, wird gemäß der Erfindung ein Steuergerät (1) der genannten Art vorgeschlagen, wobei die Überwachungseinheit (CU) erste Mittel zur Messung des Ruhestroms des Mikrocomputers (MC) aufweist, zwischen den ersten Mitteln der CU und dem MC mindestens eine Ruhestrom-Handshake-Leitung (IDDQ-HDSHK) zur Steuerung der Messung des Ruhestroms verläuft, und dass die CU zweite Mittel zur Beaufschlagung des MC mit einem Testdateneingangssignal, zur Verarbeitung des Testdateneingangssignals und zum Vergleich des entsprechenden Testdatenausgangssignals des MC mit dem entsprechenden Testdatenausgangssignal der CU aufweist und zwischen den zweiten Mitteln der CU und dem MC mindestens eine Testdatensignal-Übertragungsleitung verläuft.
(Figur 2)

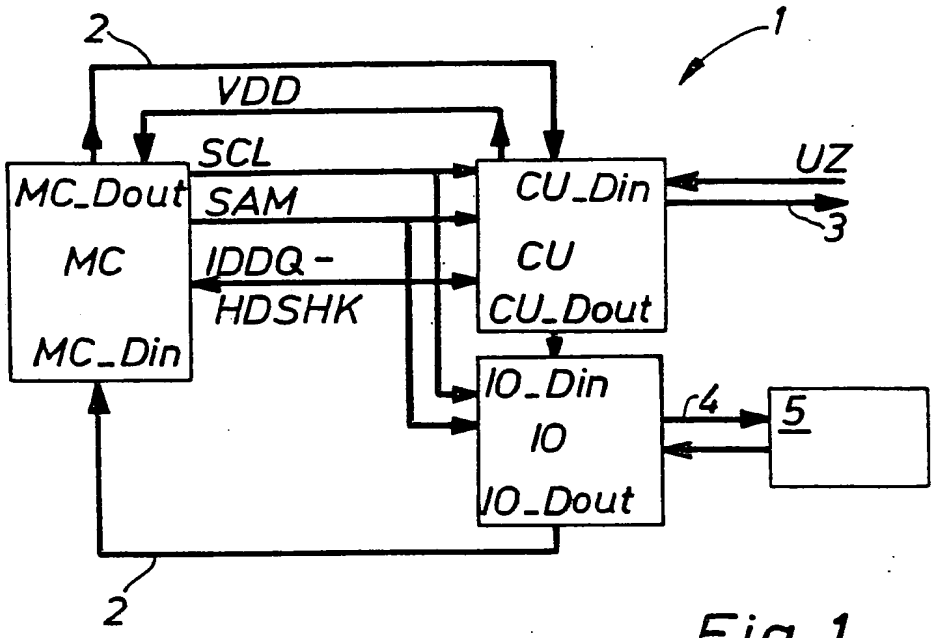
2
1
VDD
SCL
SAM
IDDQ-
HDSHK
MC_Dout
MC
MC_Din
CU_Din
CU
CU_Dout
UZ
3
IO_Din
IO
IO_Dout
4
5
2

Fig. 1

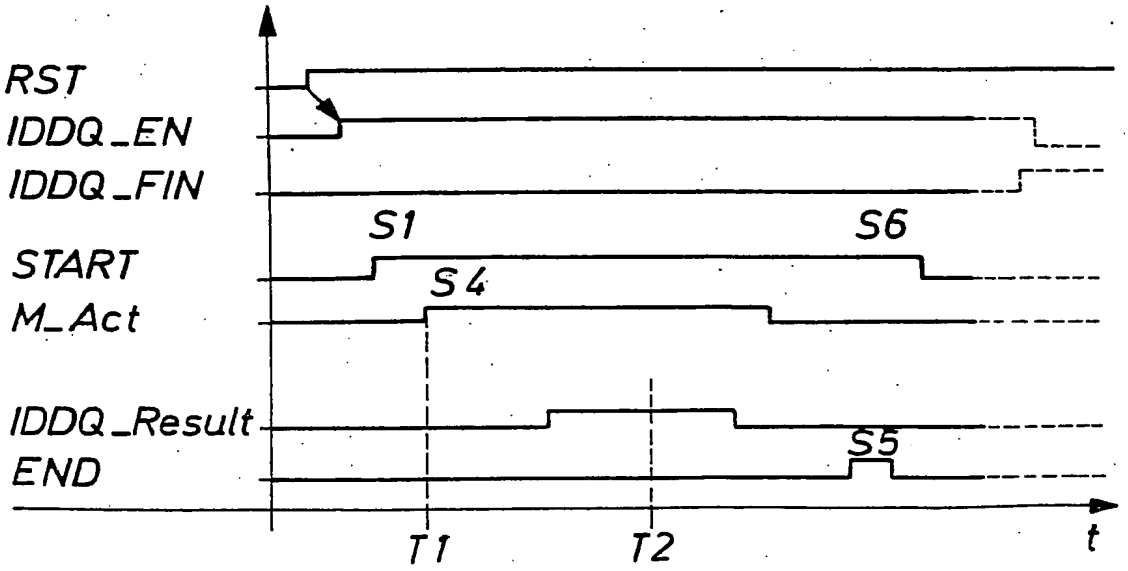
RST
IDDQ_EN
IDDQ_FIN
START
M_Act
IDDQ_Result
END
S1
S6
S4
S5
T1
T2
t

Fig. 4

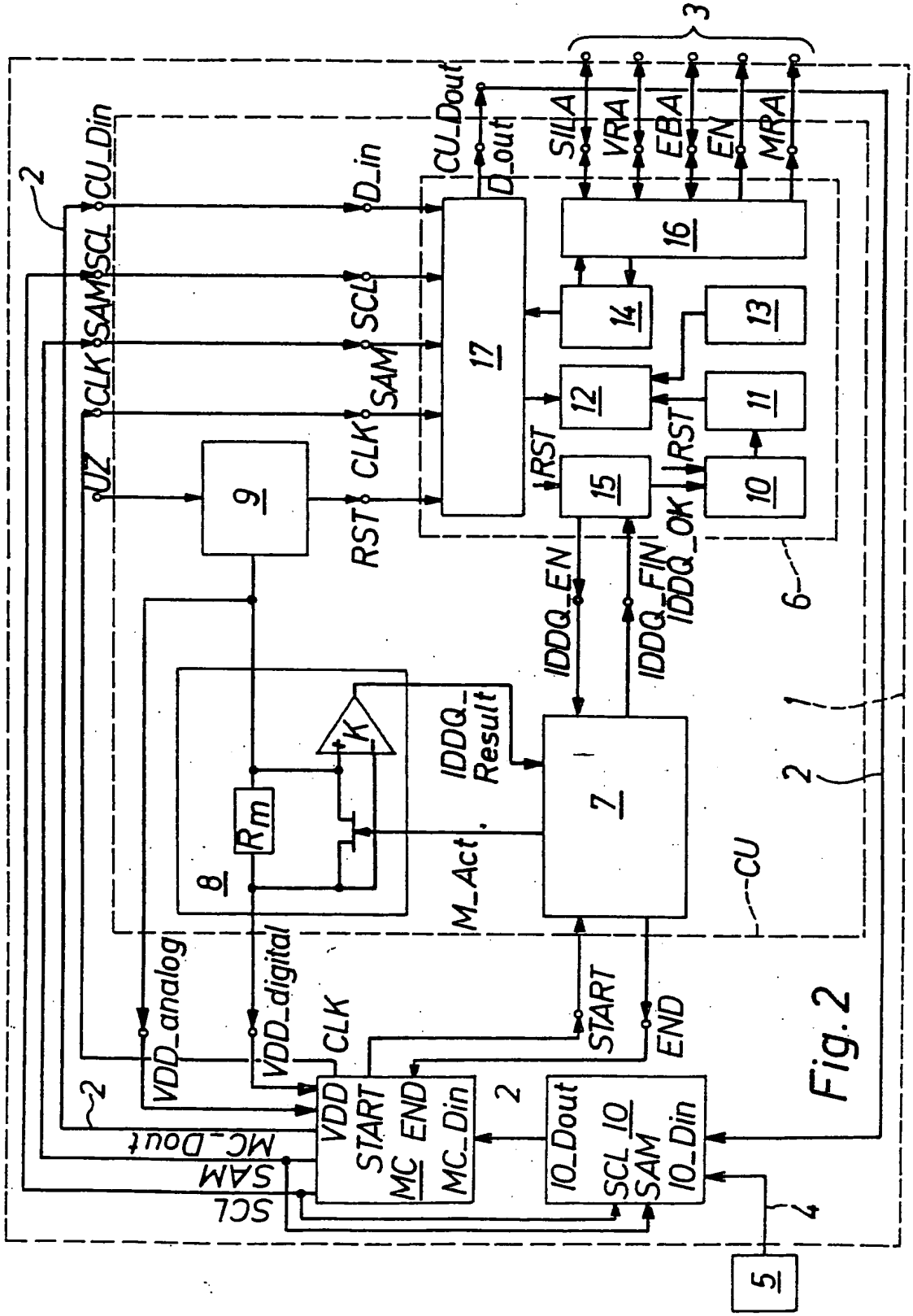
3
CU_Dout
D_out
SILA
VRA
EBA
EN
MRA
CU_Din
D_in
SCL
SAM
CLK
UZ
RST
16
17
14
13
12
11
15
10
9
IDDQ_EN
IDDQ_FIN
IDDQ_OK
6
K
IDDQ_
Result
Rm
8
7
M_Act
CU
1
2
VDD_analog
VDD_digital
CLK
START
END
VDD
START
MC_END
MC_Din
MC_Dout
SAM
SCL
IO_Dout
SCL_IO
SAM
IO_Din
4
5

Fig. 2

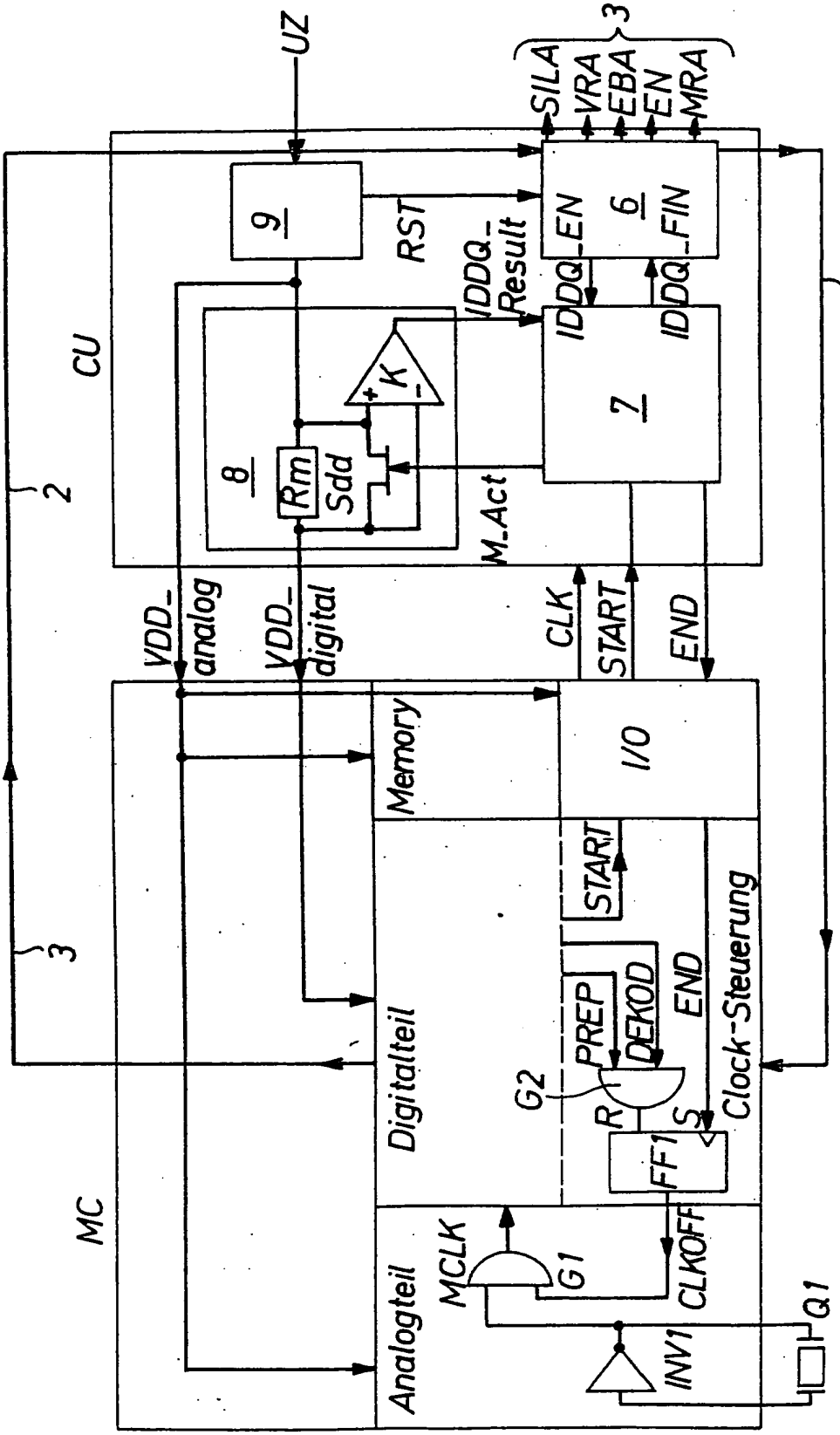
UZ
SILA
VRA
EBA
EN
MRA
3
9
RST
IDDQ_Result
6
IDDQ_EN
IDDQ_FIN
2
CU
K
8
Rm
Sdd
7
M.Act
VDD_analog
VDD_digital
CLK
START
END
Memory
I/O
START
PREP
DEKOD
END
G2
R
S
FF1
Clock-Steuerung
Digitalteil
MC
MCLK
G1
CLKOFF
Analogteil
INV1
Q1

Fig. 3